Chapter 8
A Discourse-Principle Approach to Net Neutrality Policymaking: A Model Framework and Its Application

Luca Belli, Matthijs van Bergen, and Michał Andrzej Woźniak

8.1 Introduction

The question of whether and how to protect the principle of network neutrality ("NN") is currently one of the most hotly debated topics of Internet policy around the world. As the name may already suggest, NN is essentially a non-discrimination principle that applies to the transmission of Internet traffic. It prescribes that, in principle, all Internet traffic should be transmitted on an equal basis, or at least in a manner that does not favour or disfavour particular users, applications, content, services or devices. The need to protect NN through law and policy is widely perceived as a result of the discriminatory treatment of Internet traffic which some Internet providers have begun to engage in (BEREC 2012) while others have publicly announced their wish to do so.[1] Such discriminatory treatment has the potential to restrict the freedom of Internet users to receive and impart information and use or run services and devices of their choice.

Indeed, while competition and the desire for profit-maximisation provide an important incentive for network operators to not unfairly discriminate in the transmission of Internet traffic, market failures[2] and vertical integration of operators and

[1] See *e.g.* KPN (2011) and ETNO (2012).

[2] For example, in many markets operators arguably enjoy a termination monopoly to reach the users who subscribe to their Internet access services. This enables the so-called 'Tony Soprano vision of networking' (a term credited to Tim Wu, besides 'net neutrality'), where Internet providers can extract 'protection money' from providers of online content and/or applications, by threat-

L. Belli (✉)
Fundação Getúlio Vargas Law School, Rio de Janeiro, Brazil
e-mail: luca.belli@fgv.br

M. van Bergen
ICTRecht & Leiden University, Brussels, Belgium

M.A. Woźniak
Free and Open Source Software Foundation & Warsaw Hackerspace, Warsaw, Poland

L. Belli, P. De Filippi (eds.), *Net Neutrality Compendium*,
DOI 10.1007/978-3-319-26425-7_8

online service providers appear to result in perverse incentives to violate net neutrality and to restrict or interfere with Internet users' fundamental rights and, ultimately with their freedom of choice.[3]

Discriminatory treatment of Internet traffic not only has the potential to jeopardise Internet users' right to impart and receive information, ideas and services without interference, but also to hinder competition, and to reduce the economic and social value resulting from the openness and peer to peer nature of the Internet.[4]

Over the past years, national regulators, as well as international organisations, have been producing an increasing amount of research looking for a NN formula able to sustainably preserve an open and decentralised Internet ecosystem. This article describes the process and result of a multistakeholder effort organised within the Dynamic Coalition on Network Neutrality ("DCNN"), a component of the United Nations Internet Governance Forum (IGF), established to promote debate on NN and elaborate a Model Framework for the protection of NN through policy and legislation.

The interest of a Model Framework on Network Neutrality has been stressed, since 2009, by the Council of Europe (CoE) Committee of Ministers[5] and reiterated during the CoE Multi-Stakeholder Dialogue on Network Neutrality and Human Rights (CDMSI 2013), the event that triggered the creation of the DCNN. The elaboration of the Model Framework on Network Neutrality has been coordinated by two of the authors of this paper that, at the time of the elaboration, were serving as NN experts for the CoE. One of the main goals of such effort was to deliver policy elements to the CoE Steering Committee on Media and Information Society (CDMSI), to be used for the elaboration of a NN recommendation of the CoE Committee of Ministers.[6] Important requirements for the Model Framework on NN were therefore the compliance with and promotion of international human-rights

ening to put the traffic towards their users on a slow lane, or not deliver it at all. Another problem is that the market for Internet access services is oligopolistic. In this respect, the Netherlands Bureau for Economic Policy Analysis has asserted that "one cannot be optimistic about the intensity of competition [in the telecoms sector]. Moreover, if providers make their networks "less neutral" by implementing network bias practices, the intensity of competition decreases further. " (CPB 2010) At the EU level, the Universal Service Directive (*i.e.* directive 2002/22/EC) has strengthened consumer protection, fostering better consumer information pertaining to supply conditions and tariffs in order to allow them to more easily switch providers, thus promoting competition in the electronic communications markets. However, as pointed out by BEREC several types of discriminatory practices are particularly widespread at the European level (BEREC 2012).

[3] See *e.g.* CPB (2010) and BEREC (2012).

[4] See *e.g.* van Schewick (2010), BEREC (2012), and Belli and van Bergen (2013).

[5] Particularly, para 9 of the Declaration of the Committee of Ministers on network neutrality affirms that net neutrality "should be explored further within a Council of Europe framework with a view to providing guidance to member states and/or to facilitating the elaboration of guidelines with and for private sector actors in order to define more precisely acceptable management measures and minimum quality-of-service requirements"

[6] The report containing the Model Framework was delivered to the CoE on 6 December 2013. See Belli and van Bergen (2013).

standards and also the 'scalability', which in this context means being easily implementable and applicable across different national legal systems.

This article will briefly describe the conceptual framework that led to the elaboration of a net neutrality policy-blueprint (Sect. 8.2) and the participatory process put in place by the DCNN in order to craft the Model Framework (Sect. 8.3). Lastly, we will provide the result of such process and elaborate on its concrete application (Sect. 8.4). The goal of this paper is, on the one hand, to highlight that open and participatory processes can be regarded as a viable way to develop sustainable Internet policy and, on the other hand, to provide a concrete example of such processes and their potential outcomes. The establishment of the DCNN aimed at channelling expertise coming from a variety of stakeholders towards the creation of a sustainable policy blueprint. The main goal of the Model Framework is to help clarify the NN debate and to propose a policy suggestion aimed at preserving the ability of every Internet user to freely receive and impart information as well as innovation via the Internet. To this end, the first article of the Model Framework aims at bridging a dialectic lacuna, by precisely defining the network neutrality principle. Consequently, the Model delineates the limits of the NN principle as well as the criteria according to which it should be applied. Furthermore, the Model suggests an enforcement mechanism that seems essential to implement such a crucial principle in an appropriate fashion.

8.2 A Discourse-Principle Approach

According to Jürgen Habermas' discourse principle, the only norms that one can claim to be valid are those meeting—or having the possibility to meet—the approval of all the participants in a practical discourse. Hence, Habermas argues that norms' legitimacy should not be based on their "formal-semantic properties" but should rather be guaranteed by the formal conditions that allow "rational will formation" through participation in this discourse.[7]

However, the philosopher acknowledges that, in spite of how sophisticated can be the efforts to achieve a consensual rule on a purely rational basis, human beings' lack of "perfect knowledge" inexorably leaves them in a state of uncertainty regarding whether the rules elaborated by them have truly been crafted according to the discourse principle. For this reason the most suitable solution—or the one with the least hindrance, depending on the point of view—is to undertake a participatory process through which the elaboration of the rule is legitimised by participants' free contribution on an equal footing,[8] in order to put in place "a cooperative search for truth, where nothing coerces anyone except the force of the [most persuasive] argument".[9]

[7] See Shelly (1993), pp. 65–67.

[8] Here, the expression "equal footing" should be interpreted as lack of negative discrimination with regard to the possibility to participate in a debate.

[9] See Habermas (2001), p. 198.

To foster the aforementioned Habermasian approach to policy development, all interested individuals should have the possibility to express their opinions and provide their inputs through transparent and participatory processes. Openness and transparency seem essential preconditions for the consideration of the wider number of standpoints as well as possible externalities linked to a specific policy subject (Belli 2015a, b). To this latter extent, Froomkin has stressed that the achievement of the Habermasian practical discourse depends on how closely the participants to this collaborative effort manage to approach "an ideal in which (1) all voices in any way relevant get a hearing, (2) the best arguments available to us given our present state of knowledge are brought to bear, and (3) only the unforced force of the better argument determines the 'yes' and 'no' responses of the participants".[10] However, it is important to note that only in an ideal—and particularly difficult to realise—situation it is possible to fulfil completely the conditions above. Therefore, considering the practical difficulties to realise an ideal practical discourse, "something less than the "best" might also be a practical discourse".[11]

The Internet standards elaboration process developed by the Internet Engineering Task Force (IETF), can be argued to form such a near fulfilment of the practical discourse conditions. This process is open to every interested Internet user and based on the collaborative development of Requests for Comments (RFCs) through online and onsite interactions taking place via publicly archived mailing-lists or during open workshops. The purpose of the mailing-list interaction is to facilitate the participatory process that leads to the crystallisation of "rough consensus" through the confrontation of rational arguments. In this way, the proposed standards are commented and refined in order to become draft-standards, ready to be adopted uniquely by reason of their rational efficiency.[12] Indeed, the IETF standardisation process is traditionally based on "rough consensus and running code." (Hoffman 2012) The content of the draft standards—defined "Internet Drafts"—is defined by the IETF working groups through a "rough consensus" process, whose aim is to let the dominant view of the working group emerge in the form of a general sense of agreement (Bradner 1998).

Once consensus emerge within the IETF working group, the Draft may acquire the status of Internet Standard only when all IETF members are given the possibility to comment on it through a "Last Call" for comments (Bradner 1996) and it is demonstrated that it can empirically "run" *i.e.* the technical specifications have reached technical maturity and can be implemented in multiple interoperable software applications. Such requirements are certified by the IETF Internet Engineering

[10] See Froomkin (2003), p. 771.

[11] *Ibid*., p. 776.

[12] Although Internet standards are mainly adopted by reason of their efficiency, it has been eloquently demonstrated that they have highly political connotations. To this extent, Laura DeNardis highlights that "[…] protocols are political. They control the global flow of information and make decisions that influence access to knowledge, civil liberties online, innovation policy, national economic competitiveness, national security, and which technology companies will succeed." See: DeNardis (2009), p. 6.

Steering Group (IESG) that encompasses the IETF Area Directors and whose approval allows the draft to be published as an official IETF standard, *i.e.* a RFC, by the RFC Editor. Lastly, the standards are voluntarily adopted by market players, such as network operators, software developers or online service providers.

It is important to note that the abovementioned process, which has proved reliable for the elaboration of technical standards, may be reproduced for the elaboration of policy standards or regulatory models. To this end, open working groups can be created to analyse specific policy subjects rather than technical ones and may interact via mailing-list and in physical meeting to develop policy and regulatory proposals through rough consensus processes. Such proposals may subsequently be approved, if deemed as "runnable"—i.e. concretely applicable within national legal systems—and voluntarily adopted by national regulators or inspire legislators and international organisations' policy-making efforts. In the light of this possibility, the IETF open standardisation process has been reproduced within the DCNN to conceive a model framework that could act as an open NN standard. The goal of this experiment was to elaborate a policy blueprint that could serve as an 'open regulatory standard' to be voluntarily adopted by national or international policymakers. Although very few IGF Dynamic Coalitions have produced concrete outputs so far, the reproduction of the IEFT modus operandi within an IGF Dynamic Coalition is not prohibited and the elaboration of policy or regulatory standards is, therefore, possible and delegated to each coalition's self-organisation.

8.3 A Net Neutrality Policy-Blueprint

As it has been pointed out in Part I, the participatory process put in place through open, inclusive and transparent email interaction has the potential to make the Habermasian practical discourse a (close) reality. Indeed, although mailing-list debates have obvious benefits and disadvantages,[13] it cannot be denied that they can be utilised as true debate-arenas, aimed at facilitating a "rational-will formation" process via open debates, which may be a close approximation of the Habermasian practical discourse.

Such a process is particularly beneficial to analyse the potential externalities that may be determined by specific Internet policies while considering the good (and bad) practices already adopted at both national and international level. The consideration of the various facets of a policy issue through an open and multistakeholder dialogue has indeed the potential to allow the elaboration of "scalable and innovation-enabling"[14] policies. The DCNN has therefore been established in order to transpose the practical discourse approach that characterises Internet standardisa-

[13] Particularly, Michael Froomkin highlights that, on the one hand, "much more parallel discourse is possible, which increases the chances of everyone having his or her say" whilst, on the other hand, merely virtual interactions make it "much easier to ignore people". See: Froomkin (2003), p. 799.

[14] See OECD (2011), p. 4.

tion into an IGF-based working group dedicated to net neutrality policy-analysis. IGF Dynamic Coalitions' self-organised, bottom-up and collaborative nature lends itself very well to the reproduction of the modus operandi that characterises the IETF working groups. Particularly, the creation of an open, inclusive and transparent discussion-platform is an essential requirement for the establishment of a dynamic coalition and, at the same time, a fundamental precondition to foster the confrontation of arguments leading to the formation of the rational will. Such open and multistakeholder approach is generally considered as beneficial for the development of consensus-based internet policies (OECD 2011) and seems particularly valuable for the elaboration of an efficient NN framework. Indeed, the NN debate is at the crossroad of highly contentious technical, economic and social issues (Marsden 2010; Belli and De Filippi 2013) and the large spectrum of stakeholders involved in the debate emphasises the interest of analysing this issue through a participatory and multistakeholder process.

The Multi-Stakeholder Dialogue on Network Neutrality and Human Rights, a conference organised under the auspices of the Council of Europe in May 2013 (CDMSI 2013), demonstrated the interest of a multi-faceted analysis of the NN debate and offered the participants the possibility to organise the inception of the DCNN. The CoE conference shed light on the Internet-traffic-management (ITM) techniques' potential to jeopardise the full enjoyment of fundamental rights while conferring network operators a true position of gatekeepers. The goal of the DCNN was indeed the creation of an open and multistakeholder working group able to produce a model regulatory framework protecting NN. In the view of the CoE conference participants, the elaboration of a model framework would be instrumental to provide concrete guidance on the protection of internet users fundamental rights whilst preserving the "public service value of the Internet" (CDMSI 2013).[15]

The DCNN was established with the goal of providing a discussion platform—open to all interested stakeholders—for the elaboration of a Model Framework on Network Neutrality. To this end the DCNN mailing-list has been publicly advertised (Belli 2013) and opened to any interested stakeholder. Mailing-list subscribers[16] participate on an equal footing in spite of their DCNN membership,[17] and can be categorised in five stakeholders groups: governmental entities; private-sector entities; non-governmental organisations; technical community; and academia. Mailing-list's discussions have been moderated by a coordinator, acting as an IETF working group chair, and only one "on-line vote" has been called for, in order to solve a terminology controversy.[18] Lastly, in the interest of transparency, the DCNN mailing-list archives have been kept public.

[15] See Council of Europe (2007).

[16] The total list-members number has evolved from 12, on 1st August 2013, to 82 on 1st October 2013.

[17] A complete list of DCNN members is available on http://www.networkneutrality.info/members.html.

[18] The vote was aimed at democratically choosing between Internet Access Provider (IAP), Internet Service Provider (ISP) or Internet Connectivity Provider (ICP). 74, 4 % of voters expressed a preference for the term ISP.

The first draft model framework has been elaborated utilising elements from two model laws, submitted by Luca Belli and Matthijs van Bergen to the Multi-Stakeholder Dialogue on Network Neutrality and Human Rights. Subsequently, two comment periods—the first one lasting 30 days and the second one 10—have been organised in order to reply to allow all interested stakeholder to participate in a public consultation, initiated with a "Request for Comments" on the draft model. Lastly, a third comment period has been established to allow final remarks and objections on the consolidated version of the model. The Model Framework on Network Neutrality is, therefore, the product of an open and cooperative effort and should be considered as a "policy blueprint" providing guidance on how to safeguard network neutrality. The Model Framework has been presented at the IGF meeting of the DCNN and subsequently submitted to the CoE CDMSI, which used it as working material for the elaboration of a CoE recommendation on Network Neutrality. The use or adoption of this model framework—or parts of it—should be undertaken on a merely voluntary basis and exclusively driven by the efficiency of its provisions.[19] The text of the model framework is reproduced below together with some guidelines aimed at facilitating the comprehension of its rational as well as its application.

8.4 The Model Framework and Its Application

The main goal of the Model Framework is to help clarify the NN debate and to present a way forward for NN regulation. To this end, the first article of the Model aims at bridging a dialectic lacuna, by defining the NN principle. Consequently, the Model delineates the limits of the NN principle as well as the criteria according to which it should be applied. Furthermore, the Model suggests an enforcement mechanism, essential to appropriately implement NN.

8.4.1 The Model Framework on Network Neutrality

1) *Network neutrality is the principle according to which Internet traffic shall be treated equally, without discrimination, restriction or interference regardless of its sender, recipient, type or content, so that Internet users' freedom of choice is*

[19] To this end, the European Parliament has taken inspiration from the model framework while amending the net neutrality provisions contained in the European Commission's proposal for a 'Connected Continent' regulation. Compare the Model Framework on Network Neutrality and the net neutrality provisions (particularly the net neutrality principle's definition) of the *European Parliament legislative resolution of 3 April 2014 on the proposal for a regulation of the European Parliament and of the Council laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent.*

not restricted by favouring or disfavouring the transmission of Internet traffic associated with particular content, services, applications, or devices.

2) *In accordance with the network neutrality principle, Internet service providers shall refrain from discriminating, restricting, or otherwise interfering with the transmission of Internet traffic, unless such interference is strictly necessary and proportionate to:*

   give effect to a legislative provision or court order;
   preserve the integrity and security of the network, services and the Internet users' terminal equipment;
   prevent the transmission of unsolicited communications for direct marketing purposes to Internet users who have given their prior consent to such restrictive measures;
   comply with an explicit request from the subscriber, provided that this request is given freely and is not incentivised by the Internet service provider or its commercial partner;
   mitigate the effects of temporary and exceptional network congestion, primarily by means of application-agnostic measures or, when these measures do not prove efficient, by means of application-specific measures.

3) *The network neutrality principle shall apply to all Internet access services and Internet transit services offered by ISPs, regardless of the underlying technology used to transmit signals.*
4) *The network neutrality principle need not apply to specialised services. Internet service providers should be allowed to offer specialised services in addition to Internet access service, provided that such offerings are not to the detriment of Internet access services, or their performance, affordability, or quality. Offerings to deliver specialised services should be provided on a non-discriminatory basis and their adoption by Internet users should be voluntary.*
5) *Subscribers of Internet access service have the right to receive and use a public and globally unique Internet address.*
6) *Any techniques to inspect or analyse Internet traffic shall be in accordance with privacy and data protection legislation. By default, such techniques should only examine header information. The use of any technique which inspects or analyses the content of communications should be reviewed by the relevant national data protection authority to assess compliance with the applicable privacy and data protection obligations.*
7) *Internet service providers shall provide intelligible and transparent information with regard to their traffic management practices and usage policies, notably with regard to the coexistence of Internet access service and specialised services. When network capacity is shared between Internet access services and specialised services, the criteria whereby network capacity is shared, shall be clearly stated.*
8) *The competent national regulatory authority shall:*

   be mandated to regularly monitor and report on Internet traffic management practices and usage policies, in order to ensure network neutrality, evaluate *the potential impact of the aforementioned practices and policies on fundamental rights, and ensure the provision of a sufficient quality of service and the allocation of a satisfactory level of network capacity to the Internet. Reporting should be done in an open and transparent fashion and reports shall be made freely available to the public;*

put in place appropriate, clear, open and efficient procedures aimed at addressing network neutrality complaints. To this end, all Internet users shall be entitled to make use of such complaint procedures in front of the relevant authority;

respond to the complaints within a reasonable time and be able to use necessary measures in order to sanction the breach of the network neutrality principle.

This authority must have the necessary resources to undertake the aforementioned duties in a timely and effective manner.

9) *Definitions*

The "Internet" is the publicly accessible electronic communications network of networks that use the Internet Protocol for communication with endpoints reachable, directly or through network address translation, via a globally unique Internet address.

The expression "Internet service provider" refers to any legal person that offers Internet access service to the public or Internet transit service to another ISP.

The expression "Internet access service" refers to a publicly available electronic communications service that provides connectivity to the Internet, and thereby provides the ability to the subscriber or Internet user to receive and impart data from and to the Internet, irrespective of the underlying technology used to transmit signals.

The expression "Internet transit service" refers to the electronic communications service that provides Internet connectivity between Internet service providers.

The expression "Internet traffic" refers to any flow of data packets transmitted through the Internet, regardless of the application or device that generated it.

The expression "specialised services" refers to electronic communications services that are provided and operated within closed electronic communications networks using the Internet Protocol, but not being part of the Internet. The expression "closed electronic communications networks" refers to networks that rely on strict admission control.

The expression "application-agnostic" refers to Internet traffic management practices, measures and techniques that do not depend on the characteristics of specific applications, content, services, devices and uses.

The expression "subscriber" refers to the natural or legal person who has entered into an agreement with an Internet service provider to receive Internet access service.

The expression "Internet user" refers to the natural or legal person who is using Internet access service, and in that capacity has the freedom to impart and receive information, and to use or offer applications and services through devices of their choice. The Internet user may be the subscriber, or any per-

son to whom the subscriber has granted the right to use the Internet access service s/he receives. Any legal person offering content and/or applications on the Internet is also an Internet user.

8.4.2 The Application of the Model Framework

Article 1 of the Model first defines NN and subsequently explains the aim of this principle. NN is essentially a non-discrimination principle which applies to the transmission of Internet traffic.

According to this principle, all Internet traffic is to be transmitted equally and without discrimination, restriction or interference, regardless of:

- the type or content of the traffic;
- the identity of its sender or recipient;
- the nature of the discrimination, restriction or interference (technical, financial, or otherwise).

Therefore, it may be argued that NN plays a pivotal role in enhancing freedom of choice, freedom of expression, privacy and self-determination of all Internet users, while fostering media pluralism and economic innovation (Kocsis and Weda 2013).

From these values, freedom of choice requires an additional comment. Choice can be available to subscribers on many levels—from the level of an ISP offering an Internet access service, through a level of particular service providers on the Internet, providing certain kind of services and competing with one another, down to a choice of a particular offering within a given service of a given service provider (for instance, a given article on a website). It is crucial that this choice, on all its levels, is preserved, so that subscribers can make independent choices at any time.

Specifically, choice in the form of deciding on a package of Internet access bundled with certain services (for instance, a zero-rated social network and a prioritized VoIP offering of ISP's business partners), once per a long-term contract commitment, is not conducive to the permission-less innovation principle that allowed the Internet to flourish. It is hard to anticipate when a new social network or VoIP offering eclipses the currently-popular ones, but this process—along with subscribers' choice and ability to innovate—should not be hampered by such long-term commitments that inevitably favour the established front-runners, rather than fostering the emergence of innovative services and applications.

In accordance with the network neutrality principle, ISPs must manage Internet traffic in a non-discriminatory fashion. A prime example of a non-discriminatory transmission mode is First-in, first-out, or "FIFO" transmission of Internet packets. Besides FIFO there is a multitude of other queuing and transmission policies that do not depend on the characteristics of specific applications, content, services, devices and uses. Net neutrality prescribes that ISPs must in principle apply only such "application-agnostic"[20] forms of Internet traffic management ("ITM"), while any application-specific discrimination, restriction or interference is only allowed if strictly necessary for and proportionate to any of the legitimate aims listed in article 2. The application of article 2 should be put in place through the following 'five-step test':

1) It should first be established whether or not an interference, restriction or discrimination has occurred. Any ITM that is not application-agnostic should be deemed as discrimination, restriction or interference (in short: interference);
2) the second step is to determine whether the interference in question is prescribed by the agreement between the ISP and its subscriber. If the agreement does not provide a sufficiently foreseeable ground for the interference, it is illegal. If the interference is prescribed by the agreement, we proceed to step three;
3) the third step consists in establishing whether the interference was applied for a legitimate aim. The purpose of the ITM measure must correspond with at least one of the legitimate aims, which are listed exhaustively in article 2, indents *a* to *e*;
4) the fourth step consists in determining if the measure is necessary in an open, end-to-end network. Can't the problem be properly solved at the edges? If there is no valid reason to implement a centralised measure to solve a specific problem, then the measure is not consistent with the network neutrality principle;
5) the fifth step consists in assessing the proportionality of the ITM measure. Notably, it should be evaluated whether the benefit brought by the specific measure exceeds its possible disadvantages and whether it is possible to utilise a different, less discriminatory and possibly more efficient measure in order to achieve the same purpose.

Similar to the way the European Court of Human Rights ("ECtHR") leaves a wider or smaller margin of appreciation to member states in certain situations, national courts and regulatory authorities can leave a wider or smaller margin for ISPs to decide which ITM measures are necessary and proportionate. When competition is strong, switching is easy and transparency is optimal, courts and regulators can leave a wider margin of appreciation to ISPs. When the technical community is divided concerning the discriminatory nature of a particular ITM measure, or about its efficiency or proportionality, the margin of appreciation can be left wider as well.[21]

[20] For further information about the concept of application-agnostic traffic management, see van Schewick (2012) while for a concrete application of such management see Bastian et al. (2010).

[21] As the state of the art evolves, it may at some point become clear that a certain application-specific measure which previously was broadly considered necessary and proportionate, gradually becomes inefficient and disproportionate by comparison to new measures, particularly if those measures are (more) application-agnostic. Therefore, it may be argued that the margin of appreciation becomes smaller when discriminatory ITM measures become more outdated in the light of newer, more efficient and/or more application-agnostic measures. We can imagine a 'cycle' where the same application-specific measure is first clearly necessary and proportionate, then gradually devolves and becomes less efficient at achieving its purpose compared to the state of the art, to a point where the measure is merely acceptable under the margin of appreciation for ISPs, while

It is important to note that such interference could take forms other than purely technical—for instance, subscribers could be charged more for a certain kind of traffic, or for traffic related to a certain application. One specific example is zero-rating, a practice allowing consumers to access specific services, applications or content for free by moving the cost from consumers either to the application provider or to the platform owner. As such, specific traffic (*e.g.* to/from ISP's own services, or its business partners) is favoured by the ISP by not being counted towards subscribers' monthly transfer limit, or not being charged for at all. This effectively means that the rest of subscribers' traffic is discriminated against financially. Such practices should be considered as within the scope of the Model Framework and, accordingly, should be subjected to the five-step test.

Article 2 delineates a limited number of legitimate aims for interferences. In accordance with indent a, an ISP is permitted to comply with a specific legislative provision or a court order prescribing an interference.

Indent b provides that interference may be justified if necessary to safeguard the integrity and security of the network, services and Internet users' terminal equipment. As an example, the blocking of (D)DOS traffic and malware can be mentioned.

Furthermore, it is important to note that in many European jurisdictions—at least in those within the EU—it is forbidden to send unsolicited electronic communications for direct marketing purposes, commonly referred to as "spam".[22] Although the problem of spam can also be dealt with at the 'edge', *e.g.* by filtering at the mail server, it may be considered wasteful if all spam traffic, which is said to constitute about 70–80 % of all e-mail traffic (Internet Society 2012), is first delivered to the end-point, taking up network capacity in the process, only to be discarded immediately after delivery. Therefore, filtering illegal spam at the network level forms a legitimate purpose. However, since filtering techniques always carry a risk of overblocking, the model requires the consent of the receiving subscriber in order to put in place spam filtering at the network level (which may be less granular and less precise, compared with application-level filtering). In addition, although consent of the sending subscriber to filter outgoing spam is not necessary (indeed, it seems unlikely that a spammer would ever express it), article 2 indent c requires that the least restrictive and least discriminatory method that is still sufficiently effective, is used.

If a subscriber wishes that certain application-specific ITM measures be taken by the ISP, the ISP may comply with such request, in accordance with indent d. For example, this may involve Internet access services where the ISP is explicitly requested to filter out material that the subscriber objects to for religious reasons, or that is not deemed as suitable for children. Such filtering measures can also be performed at the edges, but if the Internet user prefers that the ISP takes care of this task, and the ISP offers this functionality, this should be allowed. It is also conceivable that certain Internet users may wish to prioritise traffic relating to certain favourite applications.

finally becoming unacceptable and disproportionate in the light of the development of newer and less discriminatory alternatives.

[22] See Directive 2002/58/EC (known as the e-Privacy Directive), article 13.

The implementation of such an option (prioritisation or blocking/filtering of certain traffic per user request) in a way that leaves the Internet user in sufficiently direct control over what applications get priority and when—*i.e.* not by picking a plan that is set for the entire contract term, rather selecting applications that are to be prioritised with possibility to change it at any time, or at the very least once per billing period—would be in accordance with the model. ISPs and their commercial partners may not, however, provide any monetary or other incentives (such as discounts or free items) for Internet users to accept or request discriminatory ITM measures. Such measures should also be explicitly opt-in.

Lastly, it should be noted that, in the event of temporary and exceptional network congestion, it may be necessary to implement certain protocol-specific measures, such as prioritising traffic pertaining to real-time applications that are particularly sensitive to delay and jitter, such as (video) calling or gaming, over less time-sensitive applications, such as file sharing and e-mail. Indent *e* of article 2 leaves room for such interferences, but as it explicitly underlines: protocol-agnostic measures should be used if they are sufficiently effective in achieving the legitimate aim, whereas protocol-specific measures can only be justified if they prove more effective and/or efficient than any available application-agnostic alternatives. As such, ISPs may handle congestion giving preferential treatment protocols supporting latency-sensitive applications such as VoIP but may not prioritise only selected VoIP services.

The network neutrality principle should apply to both wired and wireless forms of Internet access services, regardless of the technology used to transmit signals (*e.g.* Ethernet, WiFi, or HDPA).

Importantly, article 2 gives no room for ‘pay-for-priority’ business models on the Internet. The mere fact that some entities may be willing to pay ISPs for implementing certain discriminations, restrictions or interferences, such as prioritising, throttling or blocking specific Internet traffic, does not constitute a legitimate aim for such interferences. However, such business models are not banned *in toto*, for they may be implemented through specialised services.

Indeed, in accordance with article 4, the network neutrality principle need not apply to specialised services, which may utilise the Internet Protocol, but which are offered on closed networks which are not part of the Internet and utilise strict access control. Examples of such services include certain IP-TV and VoIP services, often offered as a part of a ‘triple play’ package, where the subscriber of Internet access service also receives a ‘set-top’ box and digital home phones. We can also imagine certain e-health applications and other types of applications that have particularly high security requirements (a good rule of thumb is that anything connected to the Internet can be broken into or compromised), a high sensitivity to latency and jitter and a sufficiently high value to justify investments in closed networks providing specialised services besides the open Internet. In the future we may expect to see less IP-TV and VoIP services offered as specialised services, because many Internet access services now offer sufficient bandwidth to enable on demand real-time streaming of 1080p resolution HD content (content distribution networks are helpful here as well), and Skype, Vonage, Tox and other Internet-based VoIP-applications normally have better sound quality than PSTN phone lines, while their quality can be considered comparable to specialised VoIP-services, unless they are being blocked or throttled, or if there is an exceptionally high level of congestion.

However, specialised services must not be offered in such a way that would degrade the quality of Internet access services below satisfactory levels and, if capacity is shared between Internet access services and specialised services, the ISP must clearly state this and the criteria whereby this sharing takes place. To this extent, regulatory authorities have the ability to set minimum requirements for the quality of Internet access services.

It is important to stress that specialised service do not constitute a substitute for Internet access services (for instance, in a form of ISP-provided intranet, based on Network Address Translation allowing for access to the broader Internet without possibility of receiving an external IP address), nor for any service already available on the public Internet, and therefore cannot be marketed as a substitute for them. It is provided by the ISP for a fee on a specially-requested basis and offers enhanced functionalities (assured quality of service, speed or security, etc.), whose level or type is not readily available on the public Internet. It relies on strict access control, although it is offered to the public and is conveyed via physically or logically separate infrastructure from the one used to convey Internet traffic.

Physical separation implies that specialised services and Internet traffic are transported over separate equipment. Logical separation implies that specialised services and Internet traffic use the same physical equipment but the network operator dedicates specific and clearly defined resources for each type in a manner functionally equivalent to physical separation—that is resources are allocated upfront and cannot be reallocated without explicit modification of the service agreement. Such resources should also not be possible to dynamically (re)allocate.

In accordance with article 5 of the Model, all Internet users have the right to a public IP address. A public IP address enables Internet users to be more than passive consumers of online content and applications, but to be equal participants in the exchange of ideas, thoughts, information, services and applications online. This requirement can be expected to speed up adoption of IPv6 and reduce adoption of carrier-grade NAT, which may determine a variety of problems such as transforming ‘big routers in big firewalls’.[23]

Article 6 requires that any technique to inspect or analyse Internet traffic shall be limited to header information by default, and be reviewed by the relevant data protection authority if the contents of traffic are inspected or analysed.

Article 7 poses an obligation on ISPs to provide clear information about their traffic management policies. In order to provide the required transparency and information for users to base their choices for particular Internet access services on, ISPs must advertise the minimum bandwidth allocated to the Internet access service of the subscriber during the peak congestion levels on the ISPs network. This may be in addition to the theoretical maximum bandwidth levels that most ISPs currently advertise with.

[23] See *e.g.* Donley et al. (2013) and McAuley (2012).

Article 8 provides that regulatory authorities should have sufficient means and legal powers to enforce effectively net neutrality. The competent authority must regularly monitor and report on the compliance with net neutrality. The report by BEREC on traffic management practices (BEREC 2012) could serve as a basis for such reporting, while the Model additionally prescribes that regulatory authorities must be properly equipped to assess net neutrality from a human rights perspective.

Lastly, article 8(b) of the Model grants Internet users the right to file net neutrality infringement complaints with the regulatory authority as well as the competent court.

8.5 Conclusion

The Model Framework can be seen as the first regulatory standard produced by an IGF Dynamic Coalition. The value of the model framework is therefore not limited only to its content but also to its development process. Indeed, the development of the model framework has indubitably shown that the IGF can produce concrete outcomes that may be used, on a voluntary basis, to nurture national or international policy-making efforts.

However, due to the non-existence of an IGF procedure comparable to the IETF Last Call as well as to the lack of an IGF organ analogue to the IESG, the DCNN model framework cannot be considered as having the same status as an IETF standard and could be rather compared to an Internet Draft. To this end the 2014 IGF Chair's Summary called for the development of "a process that allow[s] the entire IGF community to weigh in and validate the findings of the [DCNN]."[24] Such process would be analogous to the IETF-wide Last Call, which aims at "getting the attention of people who weren't following the progress of the draft [and] get community-wide discussion on documents before the IESG considers them". In order to put in place an IGF equivalent to the Last Call process a Request for Comments aimed at developing a Policy Statement on Network Neutrality, based on the model framework, has been organised. The result of such process is described in the last article of this book.

References

Bastian, C., Klieber, T., Livingood, J., Mills, J. & Woundy, R. (2010, December). An ISP congestion management system. RFC 6057. https://tools.ietf.org/html/rfc6057#page-9

Belli, L. (2013, July 24). A new arrival in the IGF family: The dynamic coalition on network neutrality. Retrieved from http://www.medialaws.eu/a-new-arrival-in-the-igf-family-the-dynamic-coalition-on-network-neutrality/

[24] See IGF Chair (2014), p. 10.

Belli, L. (2015a, May). A heterostakeholder cooperation for sustainable internet policymaking. *Internet Policy Review*, *4*(2), 1–21.

Belli, L. (2015b). *De la gouvernance à la régulation de l'Internet*. Paris: Berger-Levrault.

Belli, L., & De Filippi, P. (Eds.). (2013, October). *The value of network neutrality for the internet of tomorrow*. 1st Report of the Dynamic Coalition on Network Neutrality.

Belli, L., & van Bergen, M. (2013). Protecting human rights through network neutrality: Furthering internet users' interest, modernising human rights and safeguarding the open internet. Council of Europe. CDMSI (2013) Misc 19.

BEREC. (2012, May 29). A view of traffic management and other practices resulting in restrictions to the open Internet in Europe. Findings from BEREC's and the European Commission's joint investigation. BoR (12) 30.

Bradner, S. (1996). The internet standards process – revision 3, request for comments: 2026.

Bradner, S. (1998). IETF Working Group Guidelines and Procedures, request for comments: 2418.

CDMSI. (2013). Council of Europe multi-stakeholder dialogue on network neutrality and human rights Strasbourg, Outcome Paper prepared by Luca Belli. CDMSI (2013) misc18E.

Council of Europe. (2007). Recommendation CM/Rec(2007)16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet.

CPB. (2010, September 23). *Memo: Response to public consultation on internet and net neutrality*. The Hague: Netherlands Bureau for Economic Policy Analysis.

DeNardis, L. (2009). *Protocol politics: The globalization of internet governance*. Cambridge, MA: MIT Press.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

Donley, C., Howard, L. Kuarsings, V., Berg, J., Doshi, J. (2013, September). Request for comments: 7021, Assessing the Impact of Carrier-Grade NAT on Network Applications. http://www.rfc-editor.org/rfc/rfc7021.txt

ETNO. (2012, September). Paper on Contribution to WCIT. ITRs Proposal to Address New Internet Ecosystem. http://www.etno.eu/datas/itu-matters/etno-ip-interconnection.pdf

Froomkin, M. (2003, January). Habermas@discourse.net: Toward a critical theory of cyberspace. *Harvard Law Review*, *116*(3), 749–873.

Habermas, J. (2001). Discourse ethics: Notes on a program of philosophical justification. In *Moral consciousness and communicative action* (Studies in Contemporary German Social Thought)

Hoffman, P. (Ed.). (2012). The Tao of IETF: A Novice's Guide to the Internet Engineering Task Force. IETF Trust. http://www.ietf.org/tao.html

IGF Chair. (2014). Connecting Continents for Enhanced Multistakeholder Internet Governance. IGF 2014 Chair' s Summary. Istanbul, Turkey.

Internet Society. (2012, October 11). Combating spam: Policy, technical and industry approaches. http://www.internetsociety.org/sites/default/files/Combating-Spam.pdf

Kocsis, V., & Weda, J. (2013, June 12). The innovation-enhancing effects of network neutrality, study commissioned by the Dutch Ministry of Economic Affairs, Amsterdam.

KPN. (2011, May 10). KPN Investor Day: Group Strategy. Strengthen – Simplify – Grow. http://pulse.companywebcast.nl/playerv1_0/default.aspx?id=12193&bb=true&swf=true

Marsden, C. (2010). *Net neutrality: Towards a co-regulatory solution*. London: Bloomsbury Academic.

McAuley, C. (2012, February 14). 3 things you need to know about carrier-grade NAT. http://blogs.ixiacom.com/ixia-blog/carrier-grade-nat-testing/

OECD. (2011). Communiqué on principles for internet policy-making. Retrieved from http://www.oecd.org/internet/innovation/48289796.pdf

Shelly, R. (1993). Habermas and the Normative Foundations of a Radical Politics. Thesis Eleven, no. 35.

Van Schewick, B. (2012, June 11). Network Neutrality and Quality of Service: What a Non-Discrimination Rule Should Look Like.

Van Schewick, B. (2010). *Internet architecture and innovation*. Cambridge, MA: MIT Press.